# IEEE-Zero Trust Security Working Group (ZTSWG) Sub-Working Group Invitation

*Dr. Ron Martin*
*Chair, IEEE Zero Trust Security Sub-Working Group*
*rlmartin1@captechu.edu*

*Dr. Jayne Suess*
*Editor, IEEE Zero Trust Security Sub-Working Group*
**jaynesuess@gmail.com**

IEEE
Φcomputer society

◈ IEEE
Advancing Technology for Humanity

# Patent and Copyright Policies



**Contribution:** any material that is presented verbally or in a recorded or written form (e.g. text, drawings, flowcharts, slide presentations, videos) in any IEEE standards development activity.

**What does this mean?** Any material you submit is intended to be considered by the Working Group to which it was submitted. The Working Group decides whether to include the material in the IEEE SA Work Product (e.g., draft standard). Once submitted, IEEE has a license to use the material.

https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/Copyright_Policy_for_Participants.pdf

# IEEE'S Patent Policy

The policy is described in Clause 6 of the *IEEE SA Standards Board Bylaws:*

https://standards.ieee.org/about/policies/opman/

Early identification of patent claims which may be essential for the use of standards under development is strongly encouraged

There may be Essential Patent Claims of which IEEE is not aware. Additionally, neither IEEE, the WG, nor the WG Chair can ensure the accuracy or completeness of any assurance or whether any such assurance is, in fact, of a Patent Claim that is essential for the use of the standard under development.

# *Project Authorization Request (PAR)*

**PAR 2887 Expiration Date:** 31 DEC 2024

"Guidance for a Zero Trust Security Capstone" ("How" Doc)

"Deliverable is the Capstone Document that will lead Sub-activities"
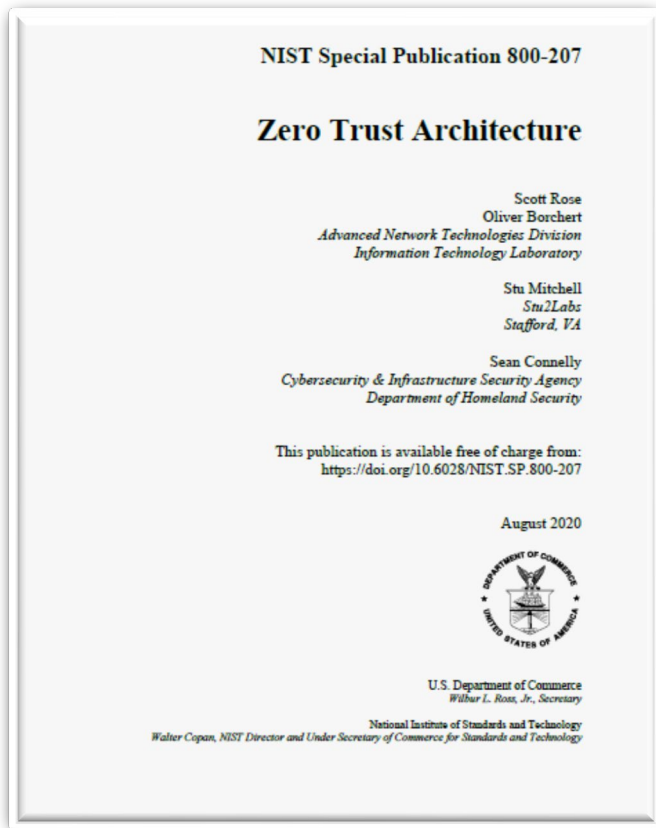
**PAR 3409 Expiration Date:** 31 DEC 2027

"Standard for a Zero Trust Security Framework" ("What" Doc).

"This Sub Working Group will develop the "What" document"

# IEEE P2887/P3409, Standard for a Zero Trust Security Framework

- **PAR 2887 Expiration Date:** 31 DEC 2024
- **PAR 3409 Approval Date:** 21 Sep 2023
- **PAR 3409 Expiration Date:** 31 Dec 2027
- **Scope:**
  - This standard provides a framework for zero trust security, including terminology, concepts, and identification of core elements

- **Summary:**
  - Serve as the IEEE ZTS (Zero Trust Security) framework (vocabulary, concepts, relevant references, etc.)
  - Bridge the ZT architecture materials (i.e., identify what is important from a security perspective)
  - Specify the minimum and optional ZTS elements ("pillars")
  - Plan to submit to ISO/IEC JTC 1/SC 27 for ISO/IEC/IEEE branding

# Zero Trust Architecture

**NIST Special Publication 800-207**

**Zero Trust Architecture**

Scott Rose
Oliver Borchert
*Advanced Network Technologies Division*
*Information Technology Laboratory*

Stu Mitchell
*Stu2Labs*
*Stafford, VA*

Sean Connelly
*Cybersecurity & Infrastructure Security Agency*
*Department of Homeland Security*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

August 2020

U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
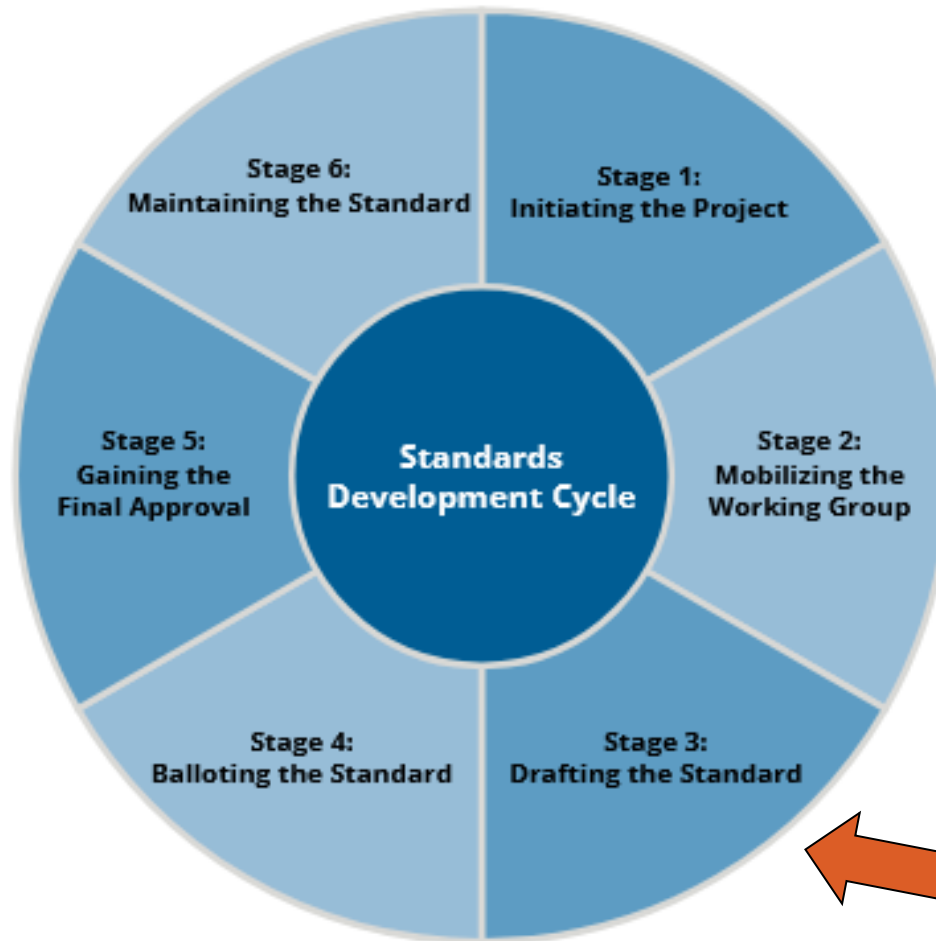*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero-trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. **Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location** (i.e., local area networks versus the internet) or **based on asset ownership** (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed

https://csrc.nist.gov/pubs/sp/800/207/final

# Standards Development Life Cycle
## IEEE SA - Drafting the Standard



**WE ARE HERE**

# IEEE P2887/P3409, Standard for a Zero Trust Security Framework Sub-Working Group

- **Work Group Meeting Schedule (Bi-Weekly)**
  - **February 8, 2024, 10:00 AM US Eastern Time**
- **Link:** https://ieeesa.webex.com/ieeesa/j.php?MTID=m595f27a52d3f0f5e98116ac60a611937
- **Scope:**
  - This Work Group will develop a candidate draft of the Zero Trust Security Guidance Standard (Stage Three)
  - The deliverable will be forwarded to IEEE Zero Trust Security Working Group (ZTSWG) for a vote to proceed to Stage Four (Balloting)
- **Summary:**
  - Service as a sub-working group member is non-voting
  - Active participation is optional; monitoring meetings is okay
  - Administrative rules and processes will be discussed

# ZTSWG Reflector Listserv

- Thank you for your interest in the P3409 Subgroup. A public email reflector has been established to provide public announcements about the WG. These announcements include teleconference information, meeting agendas, and minutes.

  To subscribe to the Public Interest Email Reflector, please only send an email to ListServ@ieee.org, containing the following text in the body of the message:

- Subscribe ZTSWG-EDITING Your FirstName Your LastName

- A confirmation email with a link will be sent to your email.  YOU MUST RESPOND TO THE CONFIRMATION.

- Once Confirmed, you will receive a welcome email

# Meeting Announcements/Agendas

- Email Distribution Lists
  - [ZTSWG-EDITING@LISTSERV.IEEE.ORG](mailto:ZTSWG-EDITING@LISTSERV.IEEE.ORG)

- A listserv message will contain:
  - Meeting Date with Agenda
  - Draft Documents for Comment
  - Advisement of Patent and Copyright Policies

- No formal Minutes

- MEETINGS WILL START AND END ON TIME!